(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－302393

(43)公開日　平成10年(1998)11月13日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｅ
			３２０Ｂ
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｄ

審査請求　未請求　請求項の数14　ＯＬ　（全 11 頁）

(21)出願番号　特願平9－107541

(22)出願日　平成９年(1997)４月24日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　加藤　岳久
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　遠藤　直樹
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　下田　乾二
神奈川県横浜市磯子区新杉田町８番地　株式会社東芝横浜事業所内

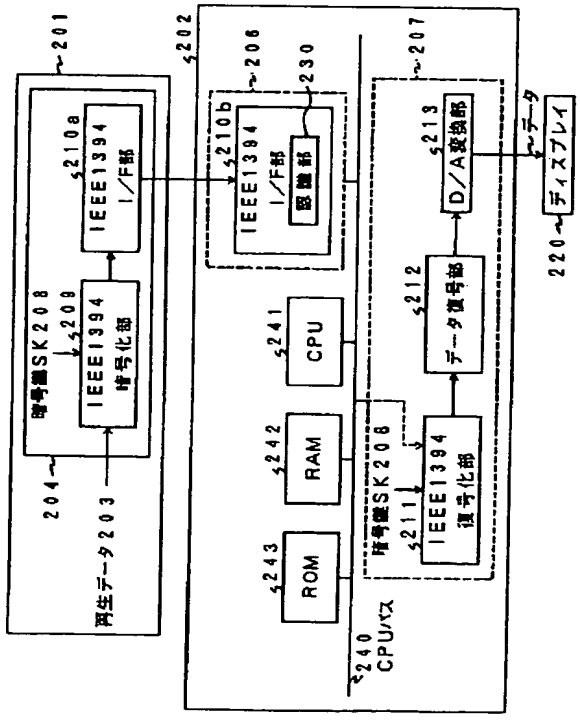
(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　不正コピーを防止する方法、及びその半導体装置並びにディジタル記録再生システム

(57)【要約】

【課題】　ＡＶ機器等と計算機等との何れもが使用され得る状況にあり、これらの機器に対して暗号化されたデータが送信される場合にあっても、ＣＰＵバス上を流れるデータのコピーによる不正なコピーを防止する。

【解決手段】　送信側と受信側とで暗号データを伝送する場合に、その送受信用インターフェースとして、専用ディジタル機器と、コンピュータ等の汎用ディジタル機器との両者を扱い可能とする統一規格に従うインターフェースを用いたディジタル機器での不正コピーを防止する方法において、受信側に用いられる機器が専用ディジタル機器であるか，汎用ディジタル機器であるかに対応して構成される統一規格の受信側Ｉ／Ｆ手段が、何れのディジタル機器に対応するかが認識され、受信側Ｉ／Ｆ手段がその対応するディジタル機器に設けられているときのみ、送信側と受信側とで正常なデータ伝送を行う不正コピーを防止する方法。



1

【特許請求の範囲】

【請求項１】　暗号化されたデータを送信する送信側と前記暗号化されたデータを受信し復号して出力する受信側との間の送受信用インターフェースとして、オーディオヴィジュアル機器等の専用ディジタル機器と、ソフトウエアでコントロール可能なＣＰＵバスをもつコンピュータ等の汎用ディジタル機器との両者を扱い可能とする統一規格に従うインターフェースを用いたディジタル記録再生システムにおいて、

前記受信側に用いられる機器が前記専用ディジタル機器であるか，前記汎用ディジタル機器であるかに対応して構成され、かつ前記送受信用インターフェースに対応して構成される受信側Ｉ／Ｆ手段と、

前記受信側Ｉ／Ｆ手段と一体にして設けられ、かつ前記受信側Ｉ／Ｆ手段が何れのディジタル機器に対応するかを認識可能とする認識手段とを備え、前記受信側Ｉ／Ｆ手段がその対応するディジタル機器に設けられているときのみ、前記送信側と前記受信側とで正常なデータ伝送を行うことを可能としたことを特徴とするディジタル記録再生システム。

【請求項２】　前記受信側Ｉ／Ｆ手段が前記汎用ディジタル機器に対応する場合において、

暗号が解読されたデータを再生出力するデータ再生出力手段と、

前記受信側Ｉ／Ｆ手段から前記ＣＰＵバスを介してデータ転送された転送先に設けられ、かつ前記ＣＰＵバスを介することなく前記データ再生出力手段にデータ出力するデータ処理手段と、

前記データ処理手段に設けられ、かつ前記暗号化されたデータを暗号解読する復号手段とを備えたことを特徴とする請求項１記載のディジタル記録再生システム。

【請求項３】　前記送信側から出力する暗号化されたデータにはデータ圧縮がかけられており、前記受信側には、圧縮されたデータを解凍する手段が設けられたことを特徴とする請求項１又は２記載のディジタル記録再生システム。

【請求項４】　前記受信側Ｉ／Ｆ手段を構成する半導体装置は、前記専用ディジタル機器に対応するものと、前記汎用ディジタル機器に対応するものとで、形状が異なり相互の交換が不可であることを特徴とする請求項１乃至３のうち何れか１項記載のディジタル記録再生システム。

【請求項５】　前記受信側Ｉ／Ｆ手段を構成する半導体装置は、前記専用ディジタル機器に対応するものと、前記汎用ディジタル機器に対応するものとで、その内部処理用のコードが異なり相互の交換が不可であることを特徴とする請求項１乃至４のうち何れか１項記載のディジタル記録再生システム。

【請求項６】　暗号化されたデータを送信する送信側と前記暗号化されたデータを受信し復号して出力する受信側との間の送受信用インターフェースとして、オーディオヴィジュアル機器等の専用ディジタル機器と、ソフトウエアでコントロール可能なＣＰＵバスをもつコンピュータ等の汎用ディジタル機器との両者を扱い可能とする統一規格に従うインターフェースを用いたディジタル機器での不正コピーを防止する方法において、

前記受信側に用いられる機器が前記専用ディジタル機器であるか，前記汎用ディジタル機器であるかに対応して構成され、かつ前記送受信用インターフェースに対応して構成される受信側Ｉ／Ｆ手段が、何れのディジタル機器に対応するかが認識され、

前記受信側Ｉ／Ｆ手段がその対応するディジタル機器に設けられているときのみ、前記送信側と前記受信側とで正常なデータ伝送を行うことを特徴とする不正コピーを防止する方法。

【請求項７】　前記受信側Ｉ／Ｆ手段が前記汎用ディジタル機器に対応する場合において、

前記受信側Ｉ／Ｆ手段にて受信された前記暗号化されたデータが前記ＣＰＵバスを介して転送され、

この転送先にて前記暗号化されたデータを暗号解読し、前記ＣＰＵバスをこれ以上介することなく解読されたデータを出力することを特徴とする請求項６記載の不正コピーを防止する方法。

【請求項８】　前記送信側から出力する暗号化されたデータにはデータ圧縮がかけられており、前記受信側にて圧縮されたデータが解凍されることを特徴とする請求項６又は７記載の不正コピーを防止する方法。

【請求項９】　暗号化されたデータを送信する送信側と前記暗号化されたデータを受信し復号して出力する受信側との間の送受信用インターフェースとして、オーディオヴィジュアル機器等の専用ディジタル機器と、ソフトウエアでコントロール可能なＣＰＵバスをもつコンピュータ等の汎用ディジタル機器との両者を扱い可能とする統一規格に従うインターフェースを用いたディジタル機器に使用される半導体装置において、

前記受信側に用いられる機器が前記専用ディジタル機器であるか，前記汎用ディジタル機器であるかに対応して構成され、かつ前記送受信用インターフェースに対応して構成されるＩ／Ｆ手段と、

前記Ｉ／Ｆ手段が何れのディジタル機器に対応するかを認識可能とする認識手段とを備えたことを特徴とする半導体装置。

【請求項１０】　前記Ｉ／Ｆ手段が前記専用ディジタル機器に対応する受信側Ｉ／Ｆ手段である場合において、前記暗号化されたデータを暗号解読する復号手段を備えたことを特徴とする請求項９記載の半導体装置。

【請求項１１】　前記専用ディジタル機器に対応するものと、前記汎用ディジタル機器に対応するものとで、形状が異なり相互の交換が不可であることを特徴とする請求項９又は１０記載の半導体装置。

【請求項１２】　前記専用ディジタル機器に対応するものと、前記汎用ディジタル機器に対応するものとで、その内部処理用のコードが異なり相互の交換が不可であることを特徴とする請求項９乃至１１のうち何れか１項記載の半導体装置。

【請求項１３】　外部より入力したデータ若しくは内部の記録媒体から読み出したデータを暗号化処理する暗号化手段と、この暗号化手段により暗号化された前記データを外部伝送路に出力する送信手段とを有する送信側機器と、

前記外部伝送路を介して前記暗号化されたデータを受信する受信手段と、この受信手段により受信した前記暗号化されたデータの復元化処理を行う復号化手段とを有する受信側機器とからなる情報提供システムにおいて、

前記送信手段は前記受信手段と交信することにより、受信側機器を認識する認識手段を備え、

前記送信手段は前記認識手段が受信側機器が送信可能な機器であると認識した場合にのみ前記データの送信を行うことを特徴とする情報提供システム。

【請求項１４】　前記受信側機器は、オーディオヴィジュアル機器等の専用ディジタル機器かソフトウェアによりコントロール可能なＣＰＵバスを有するコンピュータ等の汎用ディジタル機器の何れか一方であり、前記認識手段は受信側機器が専用ディジタル機器か汎用ディジタル機器であるかを認識することを特徴とする請求項１３記載の情報提供システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は不正コピーを防止する方法、及びその半導体装置並びにシステム、更に詳しくはディジタル化された文書、音声、画像、プログラム等の圧縮されたデータの不正コピーを防止する部分に特徴のある不正コピーを防止する方法、及びその半導体装置並びにディジタル記録再生システムに関するものである。

【０００２】

【従来の技術】最近は、マルチメディアの発展に伴つて機器のネットワーク化が進み、パーソナルコンピュータ等の汎用計算機間のみならず、オーディオ機器やビデオ機器等のオーディオヴィジュアル機器（ＡＶ機器）とのデータの送受信、ケーブルテレビや衛生放送のディジタル化等、データのディジタル化、ネットワーク化が一般的になりつつある。

【０００３】そこで、コンピュータとＡＶ機器等のディジタル機器との間でデータの送受信を行うためのディジタルインターフェース方式の統一規格が検討されている。その中の一つにＩＥＥＥ１３９４がある。このＩＥＥＥ１３９４については、例えば新エレクトロニクス文庫（２）『次世代シリアルインターフェースIEEE1394がわかる本』エレクトロニクス1997年１月号付録、オーム社、に詳述されている。

【０００４】一方、近年ディジタル記録再生機器の開発、製品化が進み、画質や音質の劣化なくデータをコピーすることが可能となっている。しかし高画質な複製は、海賊版と呼ばれる不正なコピーを増加させ、著作権が侵害されるという問題がある。このような不正なコピーは確実に防止されなければならない。というのも、インターネットやディジタルＶＴＲやＤＶＤ－ＲＡＭの出現により、ディジタル化された著作物は簡単にコピーされ、不特定多数への配布が可能となり、これによりディジタル画像の著作権者に危機感を与えているからである。

【０００５】このため、従来は、データを暗号化して通信または記録保存、読み出しをする暗号化通信または暗号化システムを用いることでこのような不正コピーを防止していた。

【０００６】

【発明が解決しようとする課題】しかしながら、ディジタル化された文書、音声、画像、プログラムなどの圧縮されたマルチメディア・データをネットワークやケーブルを介して通信を行うディジタル記録再生システム、また上記ディジタルデータを記録保存、読み出しするディジタル記録再生システムにおいては、専用機器であるＡＶ機器のみならず汎用性の高い計算機もが用いられることで次のような問題が発生する。

【０００７】すなわち、パーソナルコンピュータ（以下、パソコンともいう）のような汎用計算機を通してマルチメディア・データを再生する場合には、ＣＰＵバスを介してデータを処理するため、たとえ上記暗号化技術が用いられていても、暗号が解除された表示出力前のＣＰＵバスを流れるデータコピーすることが可能となる。

【０００８】したがって、ソフトウエア手段でパソコンを制御すれば、上記マルチメディア・データを容易にコピーすることができ、不正なコピーが可能となる。このように、ＩＥＥＥ１３９４等のインターフェースを用いて著作物を流通させた場合、パソコン等の計算機が不正コピーを助長するものになってしまう。

【０００９】また、コンピュータとＡＶ機器等とのディジタルインターフェース方式の統一規格であるＩＥＥＥ１３９４は、その汎用性から広く普及するものと予想されるが、その時にはコンピュータとＡＶ機器等との組み合わせの場合のみでなく、コンピュータのみの場合やＡＶ機器等のみの場合であってもＩＥＥＥ１３９４が使用されるものと考えられる。

【００１０】かかる状況にあっては、上記したようにパソコンを使用した場合の不正コピー防止のみならず、コンピュータとＡＶ機器との全体を考慮した不正コピー防止対策を講じなければならない。さもなければＩＥＥＥ１３９４における、コンピュータとＡＶ機器等との統一規格としての意義が失われるからである。

【００１１】本発明は、このような実情を考慮してなされたもので、ＡＶ機器等と計算機等との何れもが使用され得る状況にあり、これらの機器に対して暗号化されたデータが送信される場合にあっても、ＣＰＵバス上を流れるデータのコピーによる不正なコピーを防止することが可能な不正コピーを防止する方法、及びその半導体装置並びにディジタル記録再生システムを提供することを目的とする。

【００１２】

【課題を解決するための手段】上記課題を解決するために、請求項１に対応する発明は、暗号化されたデータを送信する送信側と前記暗号化されたデータを受信し復号して出力する受信側との間の送受信用インターフェースとして、オーディオヴィジュアル機器等の専用ディジタル機器と、ソフトウエアでコントロール可能なＣＰＵバスをもつコンピュータ等の汎用ディジタル機器との両者を扱い可能とする統一規格に従うインターフェースを用いたディジタル記録再生システムにおいて、受信側に用いられる機器が専用ディジタル機器であるか，汎用ディジタル機器であるかに対応して構成され、かつ送受信用インターフェースに対応して構成される受信側Ｉ／Ｆ手段と、受信側Ｉ／Ｆ手段と一体にして設けられ、かつ受信側Ｉ／Ｆ手段が何れのディジタル機器に対応するかを認識可能とする認識手段とを備え、受信側Ｉ／Ｆ手段がその対応するディジタル機器に設けられているときのみ、送信側と受信側とで正常なデータ伝送を行うことを可能としたディジタル記録再生システムである。

【００１３】本発明は、このような手段を設けたので、受信側に用いられる機器が専用ディジタル機器であるか，汎用ディジタル機器であるかが確実に区別されることとなり、正規な機器が用いられない場合にはデータ伝送できない。

【００１４】したがって、オーディオヴィジュアル機器等と計算機等との何れもが使用され得る状況にあっても、これらの機器に対して適切な暗号化がなされていれば、少なくともオーディオヴィジュアル機器等における不正コピーを防止できるとともに、オーディオヴィジュアル機器等と計算機等との混在使用を防止でき、ひいてはＣＰＵバス上を流れるデータのコピーによる不正なコピーを防止する手段を講じることが可能となる。

【００１５】また、請求項２に対応する発明は、請求項１に対応する発明において、受信側Ｉ／Ｆ手段が汎用ディジタル機器に対応する場合において、暗号が解読されたデータを再生出力するデータ再生出力手段と、受信側Ｉ／Ｆ手段からＣＰＵバスを介してデータ転送された転送先に設けられ、かつＣＰＵバスを介することなくデータ再生出力手段にデータ出力するデータ処理手段と、データ処理手段に設けられ、かつ前記暗号化されたデータを暗号解読する復号手段とを備えたディジタル記録再生システムである。

【００１６】本発明は、このような手段を設けたので、請求項１に対応する発明と同様な作用効果が得られる他、オーディオヴィジュアル機器等と計算機等との何れもが使用され得る状況にあり、これらの機器に対して暗号化されたデータが送信される場合にあっても、ＣＰＵバス上を流れるデータのコピーによる不正なコピーを防止することができる。

【００１７】さらに、請求項３に対応する発明は、請求項１又は２に対応する発明において、送信側から出力する暗号化されたデータにはデータ圧縮がかけられており、受信側には、圧縮されたデータを解凍する手段が設けられたディジタル記録再生システムである。

【００１８】本発明は、このような手段を設けたので、データ圧縮を行う場合にあっても、請求項１又は２に対応する発明と同様な作用効果が得られる。さらにまた、請求項４に対応する発明は、請求項１～３に対応する発明において、受信側Ｉ／Ｆ手段を構成する半導体装置は、専用ディジタル機器に対応するものと、汎用ディジタル機器に対応するものとで、形状が異なり相互の交換が不可であるディジタル記録再生システムである。

【００１９】本発明は、このような手段を設けたので、請求項１～３に対応する発明と同様な作用効果が得られる他、チップ等の半導体装置を交換することによる不正コピーを防止することができる。

【００２０】一方、請求項５に対応する発明は、請求項１～４に対応する発明において、受信側Ｉ／Ｆ手段を構成する半導体装置は、専用ディジタル機器に対応するものと、汎用ディジタル機器に対応するものとで、その内部処理用のコードが異なり相互の交換が不可であるディジタル記録再生システムである。

【００２１】本発明は、このような手段を設けたので、請求項１～４に対応する発明と同様な作用効果が得られる他、より一層確実に半導体装置を交換することによる不正コピーを防止することができる。

【００２２】次に、請求項６に対応する発明は、暗号化されたデータを送信する送信側と暗号化されたデータを受信し復号して出力する受信側との間の送受信用インターフェースとして、オーディオヴィジュアル機器等の専用ディジタル機器と、ソフトウエアでコントロール可能なＣＰＵバスをもつコンピュータ等の汎用ディジタル機器との両者を扱い可能とする統一規格に従うインターフェースを用いたディジタル機器での不正コピーを防止する方法において、受信側に用いられる機器が専用ディジタル機器であるか，汎用ディジタル機器であるかに対応して構成され、かつ送受信用インターフェースに対応して構成される受信側Ｉ／Ｆ手段が、何れのディジタル機器に対応するかが認識され、受信側Ｉ／Ｆ手段がその対応するディジタル機器に設けられているときのみ、送信側と受信側とで正常なデータ伝送を行う不正コピーを防止する方法である。

【００２３】本発明は、このような手段を設けたので、請求項１に対応する発明と同様な作用効果が得られる。また、請求項７に対応する発明は、請求項６に対応する発明において、受信側Ｉ／Ｆ手段が汎用ディジタル機器に対応する場合において、受信側Ｉ／Ｆ手段にて受信された暗号化されたデータがＣＰＵバスを介して転送され、この転送先にて暗号化されたデータを暗号解読し、ＣＰＵバスをこれ以上介することなく解読されたデータを出力する不正コピーを防止する方法である。

【００２４】本発明は、このような手段を設けたので、請求項２に対応する発明と同様な作用効果が得られる。さらに、請求項８に対応する発明は、請求項６又は７に対応する発明において、送信側から出力する暗号化されたデータにはデータ圧縮がかけられており、受信側にて圧縮されたデータが解凍される不正コピーを防止する方法である。

【００２５】本発明は、このような手段を設けたので、請求項３に対応する発明と同様な作用効果が得られる。さらにまた、請求項９に対応する発明は、暗号化されたデータを送信する送信側と暗号化されたデータを受信し復号して出力する受信側との間の送受信用インターフェースとして、オーディオヴィジュアル機器等の専用ディジタル機器と、ソフトウエアでコントロール可能なＣＰＵバスをもつコンピュータ等の汎用ディジタル機器との両者を扱い可能とする統一規格に従うインターフェースを用いたディジタル機器に使用される半導体装置において、受信側に用いられる機器が専用ディジタル機器であるか，汎用ディジタル機器であるかに対応して構成され、かつ送受信用インターフェースに対応して構成されるＩ／Ｆ手段と、Ｉ／Ｆ手段が何れのディジタル機器に対応するかを認識可能とする認識手段とを備えた半導体装置である。

【００２６】本発明は、このような手段を設けたので、請求項１に対応する発明と同様な作用効果が得られる。一方、請求項１０に対応する発明は、請求項９に対応する発明において、Ｉ／Ｆ手段が専用ディジタル機器に対応する受信側Ｉ／Ｆ手段である場合において、暗号化されたデータを暗号解読する復号手段を備えた半導体装置である。

【００２７】本発明は、このような手段を設けたので、請求項９に対応する発明と同様な作用効果が得られる。次に、請求項１１に対応する発明は、請求項９又は１０に対応する発明において、専用ディジタル機器に対応するものと、汎用ディジタル機器に対応するものとで、形状が異なり相互の交換が不可である半導体装置である。

【００２８】本発明は、このような手段を設けたので、請求項４に対応する発明と同様な作用効果が得られる。また、請求項１２に対応する発明は、請求項９～１１に対応する発明において、専用ディジタル機器に対応するものと、汎用ディジタル機器に対応するものとで、その内部処理用のコードが異なり相互の交換が不可である半導体装置である。

【００２９】本発明は、このような手段を設けたので、請求項５に対応する発明と同様な作用効果が得られる。さらに、請求項１３に対応する発明は、外部より入力したデータ若しくは内部の記録媒体から読み出したデータを暗号化処理する暗号化手段と、この暗号化手段により暗号化されたデータを外部伝送路に出力する送信手段とを有する送信側機器と、外部伝送路を介して暗号化されたデータを受信する受信手段と、この受信手段により受信した暗号化されたデータの復元化処理を行う復号化手段とを有する受信側機器とからなる情報提供システムにおいて、送信手段は受信手段と交信することにより、受信側機器を認識する認識手段を備え、送信手段は認識手段が受信側機器が送信可能な機器であると認識した場合にのみデータの送信を行う情報提供システムである。

【００３０】本発明は、このような手段を設けたことにより、まず、送信側機器において外部より入力したデータ若しくは内部の記録媒体から読み出したデータが暗号化手段により暗号化処理される。

【００３１】次に通信手段により、受信側機器の受信手段と交信がなされ、その認識手段によりデータ送信すべき受信側機器がどのようなものかが認識される。そして相手側の受信側機器が送信可能な機器であると認識された場合にのみ、送信手段により暗号化されたデータが外部伝送路に出力されデータ送信される。

【００３２】受信側機器では、受信手段により外部伝送路を介してこの暗号化されたデータが受信され、復号化手段にて暗号化されたデータの復元化処理が行われる。このようにして情報提供システムでは、データ伝送を介在する場合にあっても正しい送信側機器及び受信側機器の組み合わせのときのみデータ伝送が行われ、不用意な不正コピーを防止できることとなる。

【００３３】さらにまた、請求項１４に対応する発明は、請求項１３に対応する発明において、受信側機器は、オーディオヴィジュアル機器等の専用ディジタル機器かソフトウェアによりコントロール可能なＣＰＵバスを有するコンピュータ等の汎用ディジタル機器の何れか一方であり、認識手段は受信側機器が専用ディジタル機器か汎用ディジタル機器であるかを認識する情報提供システムである。

【００３４】本発明は、このような手段を設けたので、請求項１３に対応する発明と同様な作用効果が得られる他、特に受信側機器がコンピュータ等の汎用ディジタル機器である場合に、ＣＰＵバス上を流れるデータのコピーによる不正なコピーを防止することが可能となる。

【００３５】

【発明の実施の形態】以下、本発明の実施の形態について説明する。

（発明の第１の実施の形態）本発明にかかるディジタル

記録再生システムには、マルチメディア・データをネットワークやケーブルあるいは衛星を介して受信し再生出力する場合やＤＶＤ－ＲＡＭ，Ｄ－ＶＣＲやＣＤＲＯＭ－Ｒ等から取り出したデータを再生出力する場合等，種々の形態が考えられる。しかし、何れにしてもどこかの段階で暗号化されたデータをＩＥＥＥ１３９４により再生手段本体に伝送し、再生手段本体にて暗号を解いて再生出力することとなる。

【００３６】本実施形態では、ＭＰＥＧ２方式で圧縮されたディジタル画像をＩＥＥＥ１３９４でつながれたＤＶＤ－ＲＡＭ，Ｄ－ＶＣＲ等の記録取出部分と、記録再生ＡＶの再生部分やパソコン等の再生機器部分と間でやり取りする場合について説明する。

【００３７】まず、記録再生ＡＶにより記録再生する場合について説明する。図１は本発明の第１の実施の形態に係るディジタル記録再生システムの一例を示す構成図であり、再生機器部分にＤＶＤ－ＲＡＭ，Ｄ－ＶＣＲ等の専用ディジタル記録再生ＡＶ機器を用いる場合を示している。

【００３８】この専用ディジタル記録再生ＡＶ機器１００においては、送信機器１０１によりＤＶＤ－ＲＡＭ等から再生対象となるＭＰＥＧ２画像１０３が取出されＩＥＥＥ１３９４ケーブル１０５を介して送信される。また、送信機器１０１から送信されたデータが専用ディジタル記録再生ＡＶ機器本体である受信機器１０２によりディスプレイ１２０に再生出力されるようになっている。

【００３９】送信機器１０１は、ＤＶＤ－ＲＡＭ等からデータ圧縮されたＭＰＥＧ２画像１０３を取り出す部分（図示せず）と、ＩＥＥＥ１３９４のインターフェースの送信チップユニット１０４とから構成される。

【００４０】一方、受信機器１０２は、ＩＥＥＥ１３９４のインターフェースの受信チップユニット１０６と、ＭＰＥＧ２画像を復号するための処理部１０７とから構成される。

【００４１】送信チップユニット１０４は、ＩＥＥＥ１３９４暗号化部１０９とＩＥＥＥ１３９４Ｉ／Ｆ部１１０ａを具備する。ここで、各部１０９，１１０ａは１チップ（１ＬＳＩ，複合チップを含む）としての送信チップユニット１０４内に設けられていてもよいし、各部１０９，１１０ａはそれぞれが１チップであり、送信チップユニット１０４はこれらのチップセットからなっていていもよい。

【００４２】一方、受信チップユニット１０６は、ＩＥＥＥ１３９４Ｉ／Ｆ部１１０ｂとＩＥＥＥ１３９４復号化部１１１とを具備する。ここで、各部１１０ｂ，１１１も送信チップユニット１０４の場合と同様に、各部１１０ｂ，１１１はそれぞれが１チップで受信チップユニット１０６がこれらのチップセットであっても、各部１１０ｂ，１１１が１チップの受信チップユニット１０６内に設けられていてもよい。

【００４３】また、ＩＥＥＥ１３９４Ｉ／Ｆ部１１０ａとＩＥＥＥ１３９４Ｉ／Ｆ部１１０ｂとは、ＩＥＥＥ１３９４インターフェース規格にしたがってＩＥＥＥ１３９４ケーブル１０５を介して両者間でデータ伝送を行うものである。

【００４４】ここで、ＩＥＥＥ１３９４Ｉ／Ｆ部１１０ｂは、自己が設けられるのが専用ディジタル記録再生ＡＶ機器１００であることを認識できる構成となっている。かかる認識はＩＥＥＥ１３９４Ｉ／Ｆ部１１０ｂの認識部１３０によりなされるが、認識部１３０は、ＩＥＥＥ１３９４Ｉ／Ｆ部１１０ｂがＡＶ機器用のＬＳＩという情報を保持することで認識するようになっていてもよいし、また、ＩＥＥＥ１３９４Ｉ／Ｆ部１１０ｂがＩＥＥＥ１３９４復号化部１１１と組み合わされているということから認識するようになっていてもよい。前述の認識方法は、ＩＥＥＥ１３９４Ｉ／Ｆ部１１０ｂとＩＥＥＥ１３９４復号化部１１１とが別々のチップとなっているときに特に有効であり、後述の方法はこれらが一体のチップとなっているときに特に有効である。また、その他の認識方法を用いてもよい。

【００４５】次に、ＩＥＥＥ１３９４暗号化部１０９とＩＥＥＥ１３９４復号化部１１１とによる再生データ１０３の暗号化及び復号化について説明する。まず、送信機器１０１内において、ＭＰＥＧ２画像データ１０３は暗号鍵Ｓｋ（１０８）を用いてＩＥＥＥ１３９４暗号化部１０９により暗号化される。暗号化方式はＤＥＳやＩＤＥＡ等のブロック暗号でも構わないし、ストリーム暗号、公開鍵暗号でも構わない。本実施形態では、暗号化する鍵と復合化する鍵とが同じである共通鍵暗号方式を用いるものとする。なお、公開鍵方式の場合は、受信機器１０２から公開鍵を送ってもらい、受信機器１０２の公開鍵で暗号化すれば良い。この場合、受信機器１０２は自分が保持している秘密鍵により暗号を解くことになる。

【００４６】暗号化されたデータは、ＩＥＥＥ１３９４Ｉ／Ｆ部１１０ａにおいてＩＥＥＥ１３９４で規定されたフオーマットにされる。ＩＥＥＥ１３９４ケーブル１０５を介して受信機器１０２へ送られる。受信機器１０２ではＩＥＥＥ１３９４Ｉ／Ｆ部１１０ｂにおいてデータを受け取り暗号鍵Ｓｋ（１０８）を用いてＩＥＥＥ１３９４復号化部１１１において復号される。

【００４７】さて、ここでＩＥＥＥ１３９４Ｉ／Ｆ部１１０ａからＩＥＥＥ１３９４Ｉ／Ｆ部１１０ｂへの正常なデータ伝送が実施できるのは、これらが専用ディジタル記録再生ＡＶ機器用のＩ／Ｆセットとして正規なものが装着されているからである。すなわちＩＥＥＥ１３９４Ｉ／Ｆ部１１０ａとＩＥＥＥ１３９４Ｉ／Ｆ部１１０ｂとは通信時にお互いの認証を取り合うが、そのときに認識部１３０の機能によりＩＥＥＥ１３９４Ｉ／Ｆ部１

11

１０ｂがどのようなものであるかが認識され、当該Ｉ／Ｆ部１１０ｂが専用ディジタル記録再生ＡＶ機器用のＩ／Ｆ部でなければ通信が行われないようになっている。

【００４８】このようにして不正なＩＥＥＥ１３９４インターフェースチップが用いられた場合には、送信機器１０１～受信機器１０２間の通信ができないようになっているが、受信機器１０２において受信復号化できた場合にはさらに以下のように処理される。まず、復号されたＭＰＥＧ２画像データはＭＰＥＧ２画像を復号するための処理部１０７において、ＭＰＥＧ２圧縮されたデータがデータ復号部１１２で解凍される。そして、解答データがＤ／Ａ変換部１１３でディジタル信号からアナログ信号に変換されて、例えばディスプレイ装置１２０へ送られ再生される。

【００４９】さて、ここで暗号鍵ＳｋをＩＥＥＥ１３９４ケーブル１０５を介してどのように共有するかについて説明する。この方法については、例えばＤＶＤ－ＲＯＭにおけるＢＵＳＫｅｙの共有方式を用いればよい。

【００５０】このＢＵＳＫｅｙの共有方式については、『ニュースレポートDVD-ROM 装置用の標準インターフェースが固まる暗号鍵の安全な交換手順を規定』，日経エレクトロニクス1996. 11. 18 (No. 676) , pp. 13～pp. 14 に詳述されている。

【００５１】この方法では、まず、受信機器１０２において乱数発生器などでチャレンジ鍵１（１０バイト長）を生成し、送信機器１０１へ送る。送信機器１０１では送られたチャレンジ鍵１でＫｅｙ１（５バイト長）を生成し、受信機器１０２では同様にチャレンジ鍵１で上記と同じＫｅｙ１を生成する。Ｋｅｙ１の生成は、一方向性関数などを用いて生成される。次に、送信機器１０１はやはり乱数発生器を用いてチャレンジ鍵２（１０バイト長）を生成し、受信機器１０２へ送る。受信機器１０２では送られたチャレンジ鍵２を用いてＫｅｙ２（５バイト長）を生成する。同様に送信機器１０１では生成したチャレンジ鍵２を用いてＫｅｙ２を生成する。こうして送信機器１０１、受信機器１０２でＫｅｙ１，Ｋｅｙ２が共有できる。そこで、このＫｅｙ１及びＫｅｙ２を用いてＢＵＳＫｅｙを生成する。以上のような手順を用いれば、ＩＥＥＥ１３９４ケーブル１０５を介して、ケーブル内を暗号化するための鍵をやり取りする必要もなくなり、安全な鍵共有を図ることが可能となる。さらに、このＢＵＳＫｅｙは毎回変わるＫｅｙ１及びＫｅｙ２を用いて作成し、有効なのは１回限りである。このようにして安全性を高めている。

【００５２】このようにして、専用ディジタル記録再生ＡＶ機器１００の場合には、パーソナルコンピュータと異なりＣＰＵバスを持たないため、暗号を復号する部分と圧縮を復号する部分と受信チップユニット１０６と処理部１０７とにわけて構成し、暗号が復号されたデータを圧縮画像の復号部１１２へ送っても構わない。しかし、図１の構成をパーソナルコンピュータへ適用すれば、暗号が復号されたデータはＣＰＵバスを経由して圧縮画像の復号部へ送られるため、ＩＥＥＥ１３９４ケーブル１０５上を暗号化する意味がなくなってしまう。

12

【００５３】そこで、再生機器部分にパーソナルコンピュータを用いる場合について説明する。図２は本発明の第１の実施の形態に係るディジタル記録再生システムの他の例を示す構成図であり、再生機器部分にパーソナルコンピュータを用いる場合を示している。

【００５４】このディジタル記録再生システムにおいては、送信機器２０１によりＤＶＤ－ＲＡＭ等から再生対象となるＭＰＥＧ２画像２０３が取出されＩＥＥＥ１３９４ケーブル２０５を介して送信される。また、送信機器２０１から送信されたデータがパーソナルコンピュータである受信機器２０２によりディスプレイ２２０に再生出力されるようになっている。

【００５５】送信機器２０１は、ＤＶＤ－ＲＡＭ等からデータ圧縮されたＭＰＥＧ２画像２０３を取り出す部分（図示せず）と、ＩＥＥＥ１３９４暗号化部２０９とＩＥＥＥ１３９４Ｉ／Ｆ部２１０ａとからなるＩＥＥＥ１３９４のインターフェースの送信チップユニット２０４とによって構成されている。

【００５６】ここで、ＩＥＥＥ１３９４暗号化部２０９，ＩＥＥＥ１３９４Ｉ／Ｆ部２１０ａ，送信チップユニット２０４は、受信機器２０２に対応するものとなっている他、図１で説明したＩＥＥＥ１３９４暗号化部１０９，ＩＥＥＥ１３９４Ｉ／Ｆ部１１０ａ，送信チップユニット１０４と同様なものとなっている。

【００５７】一方、パソコンである受信機器２０２は、ＣＰＵバス２４０に、ＣＰＵ２４１，ＲＡＭ２４２，ＲＯＭ２４３，ＩＥＥＥ１３９４のインターフェースの受信チップユニット１０６及びＭＰＥＧ２画像を復号するための処理部２０７が接続されてなっている。

【００５８】ここで、ＣＰＵ２４１は受信機器２０２を制御するものであり、ＲＡＭ２４２及びＲＯＭ２４３はＣＰＵ２４１等の動作において使用されるものである。受信チップユニット２０６は、ＩＥＥＥ１３９４Ｉ／Ｆ部１１０ｂからなっており、本実施形態では１チップ（１ＬＳＩ，複合チップを含む）から構成されている。

【００５９】ＩＥＥＥ１３９４Ｉ／Ｆ部２１０ｂには、認識部２３０が設けられており、認識部１３０は、ＩＥＥＥ１３９４Ｉ／Ｆ部２１０ｂがＡＶ機器用のＬＳＩという情報を保持することで認識するようになっていてもよいし、また、ＩＥＥＥ１３９４Ｉ／Ｆ部２１０ｂが受信チップユニット２０６においてＩＥＥＥ１３９４復号化部２１１と組み合わされていないということから認識するようになっていてもよい。さらにその他の方法でもよい。

【００６０】処理部２０７は、ＩＥＥＥ１３９４復号化部２１１と、データ復号部２１２と、Ｄ／Ａ変換部２１

３とからなっており、データ復号部２１２及びD／A変換部２１３は、図１に示すデータ復号部１１２及びD／A変換部１１３と同様に構成されている。

【００６１】ＩＥＥＥ１３９４復号化部２１１は、暗号を解読し復号化する機能としては図１のＩＥＥＥ１３９４復号化部１１１と同様であるが、その位置が受信チップユニット２０６でなく処理部２０７に配置されている。

【００６２】送信機器２０１から受信機器２０２へのデータ送信における暗号化については、ＤＥＳやＩＤＥＡ等のブロック暗号や、ストリーム暗号、公開鍵暗号でも構わない。本実施形態では、専用ディジタル記録再生ＡＶ機器１００の場合と同様、暗号化する鍵と復号化する鍵とが同じである共通鍵暗号方式を用いるものとし、暗号鍵の共有は上記したＤＶＤ－ＲＯＭにおける鍵共有方式と同様な方式を用いるものとする。

【００６３】このように構成されるパソコンを含むディジタル記録再生システムにおいては、まず、ＤＶＤ－ＲＡＭ等から取り出されたＭＰＥＧ２画像データ２０３がＩＥＥＥ１３９４暗号化部２０９にて暗号化され、専用ディジタル記録再生ＡＶ機器１００の場合と同様にＩＥＥＥ１３９４Ｉ／Ｆ部２１０ａから受信機器２０２のＩＥＥＥ１３９４Ｉ／Ｆ部２１０ｂに送信される。

【００６４】ここで暗号化されたデータは、ＣＰＵバス２４０を経由して処理部２０７へ送られる。したがって、ＣＰＵバス２４０上を流れるデータをコピーしても、データには暗号がかかっており、また、暗号化に用いた鍵（ＢＵＳＫｅｙ）も上述の通り一時的なものである。したがって、ＣＰＵバス２４０上を流れるデータのコピーでは、当該データを再生できず、後に同データを処理部２０７へ送ったとしてもＢＵＳＫｅｙが一時的なものであるため再生することは不可能である。

【００６５】一方、正規にＣＰＵバス２４０を経由して送られた暗号化されたデータは、送信機器２０１と共有された暗号鍵Ｓｋ（２０８）を用いて復号化部２１１において復号される。復号されたＭＰＥＧ２画像データはデータ復号部２１２で解凍され、D／A変換部２１３でディジタル信号からアナログ信号に変換されて、ディスプレイ装置２２０などへ送られる。

【００６６】ところで上記場合に、ＩＥＥＥ１３９４Ｉ／Ｆ部２１０ａからＩＥＥＥ１３９４Ｉ／Ｆ部２１０ｂへの正常なデータ伝送が実施できるのは、これらに正規なものが装着されているからである。具体的にはパソコンやワークステーション等のソフトウエアでコントロール可能なＣＰＵバスをもつ機器を有するディジタル記録再生システム用のＩ／Ｆセットとして正規なものということである。すなわち専用ディジタル記録再生ＡＶ機器１００の場合で説明したように、ＩＥＥＥ１３９４Ｉ／Ｆ部２１０ａとＩＥＥＥ１３９４Ｉ／Ｆ部２１０ｂとは通信時にお互いの認証を取り合うが、そのときに認識部２３０の機能によりＩＥＥＥ１３９４Ｉ／Ｆ部２１０ｂがどのようなものであるかが認識される。そして、当該Ｉ／Ｆ部２１０ｂがパソコン等を用いたディジタル記録再生システム用のＩ／Ｆ部でなければ通信が行われないようになっている。

【００６７】このように、ＩＥＥＥ１３９４インターフェースように、コンピュータとＡＶ機器等との統一規格であるインターフェースを用いた場合には、ディジタルデータの再生機器部分としては、パソコン等で代表されるソフトウエアでコントロール可能なＣＰＵバスをもつ機器が用いられる場合と、このようなＣＰＵバスをもたない機器が用いられる場合に大別される。図１に示すシステムは前者の再生機器部分が用いられる場合であり、図２に示すシステムは後者の再生機器部分が用いられる場合である。これらの違いは各認識部１３０，２３０により区別され、それぞれ対応するＩ／Ｆ部１１０ｂ，２１０ｂが用いられるときのみ正常に動作する。このような区別を確実に行うことによりコンピュータとＡＶ機器等のいずれも接続できるＩＥＥＥ１３９４インターフェースにおいて、再生機器部分にコンピュータとＡＶ機器のいずれを用いての確実に両者を区別し、かつそれぞれに対応するやり方で不正コピーを防止できることとなる。

【００６８】上述したように、本発明の実施の形態に係るディジタル記録再生システム及び不正コピーを防止する方法は、コンピュータ等とＡＶ機器等のディジタル機器何れかに対応したＩＥＥＥ１３９４Ｉ／Ｆ部１１０ｂ，２１０ｂと、ＩＥＥＥ１３９４Ｉ／Ｆ部１１０ａ，１１０ｂに設けられかつＩ／Ｆ部手段１１０ｂ，２１０ｂが何れのディジタル機器に対応するかを認識可能とする認識部１３０，２３０とを具備し、Ｉ／Ｆ部がその対応するディジタル機器に設けられているときのみ、送信機器１０１，２０１と受信機器１０２，２０２間で正常なデータ伝送を行うようにしたので、ＡＶ機器等と計算機等との何れもが使用され得る状況にあり、これらの機器に対して暗号化されたデータが送信される場合にあっても、ＣＰＵバス上を流れるデータのコピーによる不正なコピーを防止することができる。

【００６９】このように専用の記録再生ＡＶ機器と汎用計算機とで受信ユニットを互換性をなくして汎用計算機のＣＰＵバス２４０上を流れるデータをコピーすることによる不正なコピーを防ぐことができる。

【００７０】また、本実施形態の半導体装置は、ＩＥＥＥ１３９４Ｉ／Ｆ部１１０ｂ，２１０ｂに認識部１３０，２３０が設けられたチップを用いたので、当該半導体装置を使用することで上記効果を得ることができる。

【００７１】なお、本実施形態では、Ｄ－ＶＣＲ等の記録機器と、記録再生ＡＶ本体やパソコン等の再生機器と間でデータ伝送する場合について説明したが、本発明はこのような場合に限られるものではなく、例えばネット

ワークや衛星通信を介してデータが伝送されてくる場合にも適用できる。例えば衛星からＭＰＥＧ２圧縮され暗号化されたデータを受信する場合には送信機器１０１，２０１に対応するものとしてセットボックス（ＳＴＢ）が設けられることとなるが、セットボックス～受信機器１０２，２０２間のＩＥＥＥ１３９４によるデータ伝送は、本実施形態の場合と同様に考えることができる。

【００７２】また、本発明は、例えばネットワークの接続先が送信機器１０１，２０１に対応し、再生画像等使用者側には受信機器１０２，２０２に対応する記録再生ＡＶ本体やパソコン等の再生機器のみがあるような場合にも適用できる。

（発明の第２の実施の形態）上記実施形態で説明したように、専用ディジタル記録再生ＡＶ機器本体とパーソナルコンピュータとで構成を変えたとしても、パソコンを用いる場合に不正コピー者によって、送信チップユニット２０４と受信チップユニット２０６のチップセットを送信チップユニット１０４と受信チップユニット１０６のチップセットに交換されてしまう場合も考えられる。

【００７３】本実施形態は、このような場合に対応するものである。図３は本発明の第２の実施の形態に係るディジタル記録再生システムに使用されるチップ形状の例を示す図である。

【００７４】なお、同図に示すチップ形状を除き本実施形態のディジタル記録再生システムは、第１の実施形態の場合と同様に構成されている。図３（ａ）は、専用ディジタル記録再生ＡＶ機器用の送信チップユニット１０４，Ｉ／Ｆ部１１０ａ又は受信チップユニット１０６，Ｉ／Ｆ部１１０ｂの構成例を示している。一方、図３（ｂ）は、パーソナルコンピュータを使用するシステム用の送信チップユニット２０４，Ｉ／Ｆ部２１０ａ又は受信チップユニット２０６，Ｉ／Ｆ部２１０ｂの構成例を示している。

【００７５】このように、専用ディジタル記録再生ＡＶ機器とパーソナルコンピュータとで用いられるチップの形状として、例えば足の数やボディ部の大きさや形などの形状を変えることで、チップの交換を防止できる。

【００７６】上述したように、本発明の実施の形態に係る不正コピーを防止する方法、半導体装置及びディジタル記録再生システムは、専用ディジタル記録再生ＡＶ機器とパーソナルコンピュータとで用いられるチップの形状として、例えば足の数やボディ部の大きさや形などの形状を変えるようにしたので、半導体装置であるチップの交換を防止でき、第１の実施形態で奏する効果をより一層確実なものとすることができる。

（発明の第３の実施の形態）第２の実施形態では、チップ形状を変更することでチップの交換を防止したが、本実施形態は受信機器において、ＶＴＲ等の専用ディジタル記録再生ＡＶ機器とパーソナルコンピュータとで用いられるチップの内部処理のコードを変えることにより、受信ユニット（チップ）の交換を実質的に不可能とするものである。

【００７７】具体的には、例えばアスキーコード等のチップ内の制御コマンドの割り当てを、ＡＶ機器等用とパソコン等用とで異なったものとする。このように、チップの計上による非互換性だけでなく、内部処理コマンドの違いにより非互換性を担保することができる。

【００７８】したがって、制御コマンドの割り当てが異なっているために、もし交換して使用したとすると、外部からの入力に対してチップ内の処理が異なり、正常な動作をしなくなる。そのため、たとえチップを交換できたとしても利用することは不可能である。

【００７９】上述したように、本発明の実施の形態に係る不正コピーを防止する方法、半導体装置及びディジタル記録再生システムは、専用ディジタル記録再生ＡＶ機器とパーソナルコンピュータとで使用されるチップの内部処理のコードを変えるようにしたので、半導体装置であるチップの交換を確実に防止でき、第１の実施形態で奏する効果をより一層確実なものとすることができる。

【００８０】また、本実施形態において、例えばチップにＣＰＵが入っているような場合は、言語をＺ８０とＣ言語というように異なる言語を用いることにより、上記と同様の効果を持たせることもできる。

（発明の第４の実施の形態）第２の実施形態では、チップ形状を変更し、第３の実施形態ではチップ内コードを変更することでチップの交換を防止したが、本実施形態は受信機器において、ＶＴＲ等の専用ディジタル記録再生ＡＶ機器とパーソナルコンピュータとで用いられるチップのピンにＡＶ機器等かパソコン等かを識別するピンを設けることで受信ユニット（チップ）の交換を実質的に不可能とするものである。

【００８１】具体的には、本実施例のチップは、ＬＳＩピンの一つが機器認識用のピンとなっており、このピンから入力される信号により自ＬＳＩがＡＶ機器等かパソコン等かの正しい機器に接続されたか否かを自己判定し、正しい機器に接続されていないときには動作しないように構成されている。

【００８２】例えば受信機器がパーソナルコンピュータである場合には、上記機器認識用のピンの接続先をダミーとし、ピンに対しては信号入力無しとする。一方、受信機器が専用デジタル記録再生ＡＶ機器本体である場合には、一定の信号を入力するようにする。

【００８３】したがって、上記一定の信号が入力されるか否かで、チップは自己の対応すべき機器に接続されたかを判定できる。なお、機器認識用のピンへの入力は、ＡＶ機器等かパソコン等かで上記場合と逆にしてもよいし、また例えばＨレベル、Ｌレベル信号で区別するようにする等．種々の形態が考えられる。なお、本発明は、上記各実施の形態に限定されるものでなく、その要旨を逸脱しない範囲で種々に変形することが可能である。

17

【００８４】

【発明の効果】以上詳記したように本発明によれば、ＡＶ機器等と計算機等との何れもが使用され得る状況にあり、これらの機器に対して暗号化されたデータが送信される場合にあっても、ＣＰＵバス上を流れるデータのコピーによる不正なコピーを防止することが可能な不正コピーを防止する方法、及びその半導体装置並びにディジタル記録再生システムを提供することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態に係るディジタル記録再生システムの一例を示す構成図。

【図２】本発明の第１の実施の形態に係るディジタル記録再生システムの他の例を示す構成図。

【図３】本発明の第２の実施の形態に係るディジタル記録再生システムに使用されるチップ形状の例を示す図。

【符号の説明】

１０１…送信機器

１０２…受信機器（専用ディジタル記録再生AV機器本体）

１０３…ＭＰＥＧ２画像データ

１０４…送信チップユニット

１０５…ＩＥＥＥ１３９４ケーブル

１０６…受信チップユニット

１０７…処理部

１０８…暗号鍵Ｓｋ

１０９…ＩＥＥＥ１３９４暗号化部

１１０ａ…ＩＥＥＥ１３９４Ｉ／Ｆ部

18

１１０ｂ…ＩＥＥＥ１３９４Ｉ／Ｆ部

１１１…ＩＥＥＥ１３９４復号化部

１１２…データ復号部

１１３…Ｄ／Ａ変換部

１２０…ディスプレイ

１３０…認識部

２０１…送信機器

２０２…受信機器（専用ディジタル記録再生AV機器本体）

２０３…ＭＰＥＧ２画像データ

２０４…送信チップユニット

２０５…ＩＥＥＥ１３９４ケーブル

２０６…受信チップユニット

２０７…処理部

２０８…暗号鍵Ｓｋ

２０９…ＩＥＥＥ１３９４暗号化部

２１０ａ…ＩＥＥＥ１３９４Ｉ／Ｆ部

２１０ｂ…ＩＥＥＥ１３９４Ｉ／Ｆ部

２１１…ＩＥＥＥ１３９４復号化部

２１２…データ復号部

２１３…Ｄ／Ａ変換部

２２０…ディスプレイ

２３０…認識部

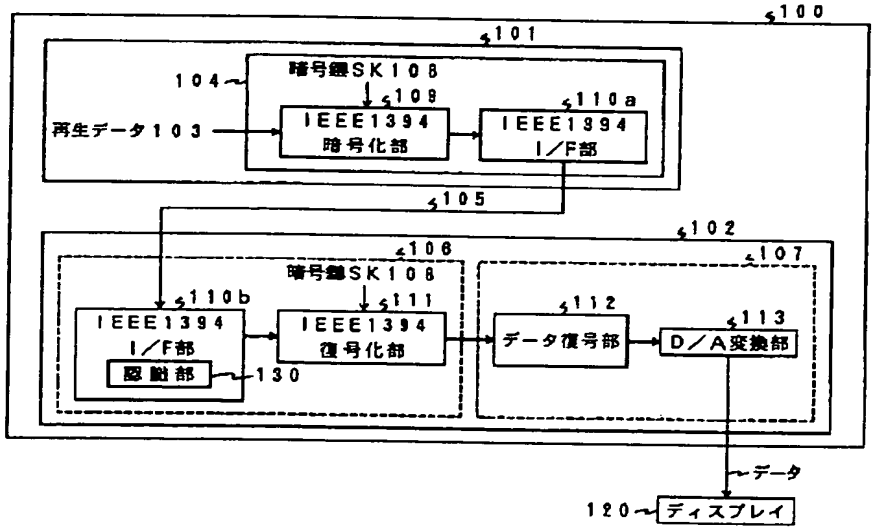
２４０…ＣＰＵバス

２４１…ＣＰＵ

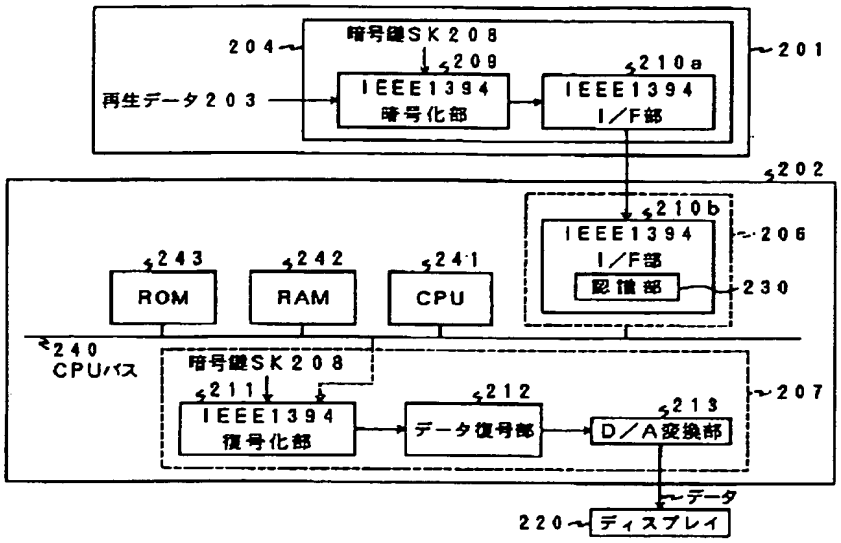
２４２…ＲＡＭ

２４３…ＲＯＭ

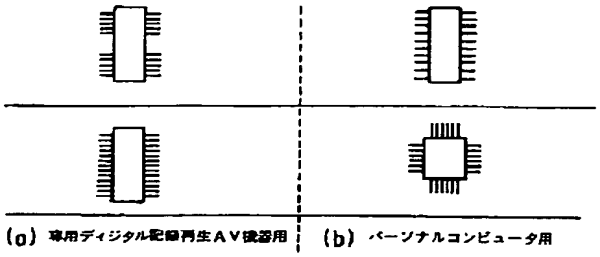
【図１】



【図２】


暗号鍵ＳＫ２０８
２０４
２０９
２１０ａ
２０１
再生データ２０３
IEEE1394 暗号化部
IEEE1394 I／F部
２０２
２１０ｂ
IEEE1394 I／F部
２０６
記憶部
２３０
２４３
２４２
２４１
ROM
RAM
CPU
２４０ CPUバス
暗号鍵ＳＫ２０８
２１１
２１２
２１３
２０７
IEEE1394 復号化部
データ復号部
D／A変換部
データ
２２０
ディスプレイ

【図３】


(a) 専用ディジタル記録再生ＡＶ機器用
(b) パーソナルコンピュータ用